Maryland HIPAA Security Rule Policy

Last Updated: 01/31/2017

Contents

1.0 Purpose 3
2.0 Document and Review History 3
3.0 Applicability and Audience 3
4.0 Policy 4
4.1 Security Standards — General Rule 4
4.2 Administrative Safeguards 4
4.3 Physical Safeguards 5
4.4 Technical Safeguards 6
4.5 Organizational Requirements 6
4.6 Documentation Requirements 7
4.7 Breach Notification 7
5.0 Exemptions 8
6.0 Policy Mandate and References 8
7.0 Definitions 8
8.0 Enforcement 9

1.0 Purpose

The Maryland Department of Information Technology is committed to managing the confidentiality, integrity, and availability of **electronic protected health information (ePHI)** created, stored, processed, and transmitted electronically via State government Information Technology (IT) networks, systems, and applications (IT Systems). Agencies considered **covered entities (CE)** under the **Health Insurance Portability and Accountability Act of 1996 (HIPAA)** must comply with the requirements of HIPAA. The Maryland Department of Information Technology (DoIT) will utilize baseline specifications as outlined by the **HIPAA Security Rule** and NIST SP 800-66.

2.0 Document and Review History

This document will be reviewed annually and is subject to revision.

Date	Version	Policy Updates	Approved By:
01/31/2017	v1.0	Initial Publication	Maryland CISO

3.0 Applicability and Audience

This policy is primarily concerned with the HIPAA Security Rule and will not cover other standards or provisions adopted through HIPAA, such as the **HIPAA Privacy Rule**, covered entities will need to comply with all relevant regulations, legislation, directives, executive orders, and laws when handling PHI.

This policy applies to ePHI stored, processed, or transmitted electronically by IT assets utilized by any Executive agency of the state of Maryland, employees of such agencies, contractors and vendors supporting such agencies, and any entities or individuals using resources owned or operated by such agencies, who qualify as a **Covered Entity (CE)** under HIPAA. Covered entities include the groups listed in the table below.

#	Covered Entity	Description
A	Healthcare Provider	A person or organization that provides patient or medical services, such as a doctor, clinics, hospital and outpatient services.
B	Health Plan	An entity that provides payment for medical services such as health insurance companies, HMOs, government health plans, and government programs that pay for healthcare such as Medicare, Medicaid, military, and veteran's programs.
C	Healthcare Clearinghouse	Entities that process nonstandard health information they receive from another entity into a standard format.
D	Business Associate	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.

4.0 Policy

This policy provides guidance for compliance with the main requirements of the HIPAA Security Rule but does not supplement, replace, or supersede the HIPAA Security Rule itself.

4.1 Security Standards — General Rule

The HIPAA Security Rule is flexible by nature and differentiates between **Required Implementation Specifications** (akin to standards) and **Addressable Implementation Specifications**. Addressable specifications are not required but must be assessed by CEs to determine whether the specification is reasonable and appropriate for their organizations.

NOTE: This policy provides guidance for compliance with required specifications of the Security Rule. Agencies are responsible for assessing addressable specifications separately and implementing them as resources, technology, and budgets allow.

4.2 Administrative Safeguards

Administrative safeguards are the actions and procedures established to manage the selection, development, implementation, and maintenance of security measures to protect ePHI and to manage the conduct of the CE's workforce relative to protecting that information.

CEs must ensure administrative safeguards are in place by meeting the requirements described in the table below.

	Name	Requirement
A	Security Management Process	Establish a formal security management process, which includes the following: ▪ Conduct risk assessments — Conduct an accurate and thorough assessment of the potential risks and vulnerabilities of ePHI held by the CE ▪ Implement a risk management program — Implement security measures sufficient to reduce risks and vulnerabilities to an appropriate level ▪ Develop and implement a sanction policy — Policy must define consequences of security violations ▪ Develop and deploy an information system activity review process — Implement procedures to regularly review records of information system activity, including audit logs, access reports, and incident reports
B	Assigned Security Responsibility	Designate an individual as the Security Officer. The Security Officer is responsible for overseeing the development of policy, implementing the policy, and monitoring to ensure compliance.
C	Workforce Security	Implement policies and procedures to ensure that all members of the workforce have appropriate (restricted) access to ePHI, and prevent those workforce members who do not require access from obtaining access to ePHI.
D	Information Access Management	Implement formal policies and procedures granting access to ePHI by isolating Healthcare Clearinghouse function. ▪ If a healthcare clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures to protect the ePHI from unauthorized access by the larger organization.

	Name	Requirement
E	Security Awareness and Training	Implement a security awareness and training program for all members of the workforce.
F	Security Incident Procedures	Implement policies and procedures to address security incidents. CEs must develop and implement procedures to respond to and report security incidents. ▪ Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents; and document security incidents and outcomes.
G	Contingency Plans	Establish and implement policies and procedures for responding to an emergency or other disturbance, e.g., fire, vandalism, system failure, or natural disaster, that damages systems housing ePHI, including: ▪ Data Backup Plan — Include procedures to create and maintain retrievable exact copies of ePHI ▪ Disaster Recovery Plan — Include procedures to restore any lost data ▪ Business Continuity Plan — Include procedures to enable continuation of critical business processes for protecting the security of ePHI while operating in emergency mode
H	Periodic Evaluation	CEs must implement policies and procedures that require periodic technical and non-technical evaluation of HIPAA Security Rule compliance against the standards initially implemented in response to environmental or operating changes that affect the security of ePHI.
I	Business Associate Contracts and Other Arrangements	Implement policy to document rules for **Business Associate** identification and process, including a written contract or other arrangement with the Business Associate that meets the standard of Organizational Requirements (see Section 4.5 below).

4.3 Physical Safeguards

CEs must ensure physical safeguards are in place by meeting the requirements listed in the table below.

#	Name	Requirement
A	Facility Access Controls	Implement policies and procedures to limit physical access to electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.
B	Workstation Use	Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI. Ensure that workstations and other computer systems used to send, receive, store or access ePHI are only used legitimately and securely.
C	Workstation Security	Implement physical safeguards for all workstations that access ePHI, restricting access to authorized users.
D	Device and Media Controls	Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility, including the following:

#	Name	Requirement
		▪ Implement policies and procedures to address the final disposition of ePHI and the hardware or electronic media on which it is stored ▪ Implement procedures for removal of ePHI from electronic media before the media are made available for reuse

4.4 Technical Safeguards

CEs must ensure technical safeguards are in place by meeting the requirements listed in the table below.

#	Name	Requirement
A	Access Controls	Implement technical policies and procedures for electronic information systems that contain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in Information Access Management (See section 4.2(D)), including procedures to: ▪ Assign a unique ID for identifying and tracking user identity ▪ Obtain ePHI during an emergency, implemented as needed
B	Audit Controls	Implement hardware, software, and procedural mechanisms that record and examine activity in information systems that contain or use ePHI.
C	Integrity Controls	Implement policies and procedures to protected ePHI from improper alteration or destruction.
D	Person or Entity Authentication	Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.
E	Transmission Security	Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.

4.5 Organizational Requirements

CEs must ensure organizational requirements are in place through the creation of business associate contracts or other arrangements. Contracts between CEs and business associates must:

- Ensure business associates implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of any and all ePHI the business associates create, receive, maintain, or transmit on behalf of the CE
- Ensure any agent, including a subcontractor, to whom the business associate provides such information agrees to implement reasonable and appropriate safeguards to protect it
- Ensure business associates report to the CE any security incident of which they become aware
- Ensure the CE has the authorization to terminate the contract if the CE determines that the business associate has violated a material term of the contract

Government entities may satisfy business associate contract requirements through other arrangements such as a **Memorandum of Understanding (MOU)** (e.g., if both the CE and business associate are government entities).

If a business associate is required by law to perform a function or activity on behalf of the CE or to provide a service as a business associate, the CE may permit the business associate to create, receive, maintain, or transmit ePHI on its behalf to the extent necessary without requiring a business associate agreement, provided that the CE attempts in good faith to obtain satisfactory assurances that administrative, physical, and technical safeguards are implemented or the CE documents the attempt and the reasons that theses assurances cannot be obtained.

4.6 Documentation Requirements

CEs must ensure documentation requirements are in place as required in the table below.

#	Name	Requirement
A	Policies and Procedures	Maintain the policies and procedures implemented to comply with the HIPAA Security Rule in written form (which may be electronic). ▪ Written documentation may be incorporated into existing manuals, policies, and other documents, or may be created specifically for the purpose of demonstrating compliance with the HIPAA Security Rule.
B	Documentation	The Security Rule requires that CEs: ▪ Retain documentation of policies, procedures, actions, activities or assessments required by the HIPAA Security Rule for six (6) years from the date of its creation or the date when it last was in effect, whichever is later ▪ Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains ▪ Review documentation periodically, and update as needed, or in response to environmental or operational changes affecting the security of ePHI

4.7 Breach Notification

The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA covered entities and their business associates to provide notification following a breach of **unsecured protected health information**. An impermissible use or disclosure of protected health information (Breach) is presumed to be a breach unless the covered entity or business associate, as applicable, demonstrates that there is a low probability that the protected health information has been compromised based on a risk assessment of at least the following factors:

- The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;
- The unauthorized person who used the protected health information or to whom the disclosure was made;
- Whether the protected health information was actually acquired or viewed; and
- The extent to which the risk to the protected health information has been mitigated.

Covered entities and business associates have discretion to provide the required breach notifications – following an impermissible use or disclosure – without performing a risk assessment to determine the probability that the protected health information has been compromised. Refer to HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414 for explicit instructions regarding breach definitions, exemptions, and notification requirements.

5.0 Exemptions

The requirements of this policy are established by Federal and Maryland laws and standards, and there are no exemptions to this policy.

6.0 Policy Mandate and References

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the DoIT Cybersecurity Program Policy mandate this policy. Related policies include:

- Account Management Policy
- Asset Management Policy
- Contingency Planning Policy
- Security Assessment Policy

7.0 Definitions

Term	Definition
Addressable Specification	Specifications outlined within the HIPAA Security Rule which CEs must assess to determine whether they are a reasonable and appropriate safeguard in the entity's environment.
Business Associate (BA)	A person or entity that performs certain functions or activities that involve the use or disclosure of protected health information on behalf of, or provides services to, a covered entity.
Covered Entities (CE)	Defined in the HIPAA rules as (1) health plans, (2) health care clearinghouses, and (3) health care providers who electronically transmit any health information in connection with transactions for which the U.S. Department of Health and Human Services has adopted standards. ▪ BA's can be considered Covered Entities.
Electronic Protected Health Information (ePHI)	Refers to any protected health information (PHI) that is covered under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) security regulations and is produced, saved, transferred or received in an electronic form.
Health Insurance Portability and Accountability Act (HIPAA) of 1996	Establishes national standards for electronic health care transactions. The two main parts of HIPAA include the Privacy and Security Rules.
HIPAA Privacy Rule	Gives an individual or a patient rights over their health information and sets rules and limits as to who can view and receive health information and records.
HIPAA Security Rule	Establishes national standards for securing patient data that is stored or transmitted electronically.

Term	Definition
Memorandum of Understanding (MOU)	A formal agreement between two or more parties. Often used by companies and organizations to establish official partnerships.
Required Specification	Specifications outlined within the HIPAA Security Rule which CEs are required to implement.
Unsecured Protected Health Information	Unsecured protected health information is protected health information that has not been rendered unusable, unreadable, or indecipherable to unauthorized persons through the use of a technology or methodology specified by the Secretary in guidance.

8.0 Enforcement

Failure to comply with HIPAA can result in civil and/or criminal penalties (42 USC § 1320d-5). Civil Penalties range from $100 per violation to $50,000 per violation, with annual limits dependent on the nature and extent of the violation and the nature and extent of the harm resulting from the violation.

If DoIT determines that an agency is not compliant with the HIPAA Security Rule Policy, the agency will be given sixty (60) days to become compliant according to the requirements in this policy. After such time, if the agency remains out of compliance the Secretary of Information Technology will be notified and remediation will be mandated. If a complaint is reported to US Department of Health and Human Services, the Office of Civil Rights (under authority of DHHS) may investigate and conduct a compliance audit. Should a complaint describe an action that could be a violation of the criminal provision of HIPAA (42 U.S.C. 1320d-6), the Office of Civil Rights may refer the complaint to the Department of Justice for investigation resulting in possible monetary penalties.

Any personnel attempting to circumvent the requirements of HIPAA, such as willfully or negligently disclosing ePHI, will be investigated as a security violation and subject to disciplinary action which may include written notice, suspension, termination, and possible criminal and/or civil penalties.